UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 4:19 CR 980 HEA (JMB)
	)	
HAITAO XIANG,	)	
	)	
Defendant.	)	

REPORT AND RECOMMENDATION AND
ORDERS OF UNITED STATES MAGISTRATE JUDGE

Currently before the Court are the following motions filed on behalf of Defendant Haitao Xiang: (1) Motion for Early Trial Subpoenas [ECF No. 79]; (2) Motion to Suppress Evidence [ECF No. 93]; and (3) Motion for Disclosure of Expert Witnesses [ECF No. 95]. The government opposes Xiang's Motion to Suppress and Motion for Disclosure and did not respond to Xiang's Motion for Early Trial Subpoenas. Pretrial motions were referred to the undersigned United States Magistrate Judge. See 28 U.S.C. § 636(b).

INTRODUCTION AND PROCECURAL BACKGROUND

Xiang was initially charged by felony complaint on November 15, 2019. Thereafter, a Grand Jury in our District returned a multi-count indictment against Xiang. According to the Indictment, Xiang is a citizen of the People's Republic of China ("PRC") who was formerly a permanent legal resident of the United States. While in the United States, Xiang worked for Monsanto and The Climate Corporation ("TCC"), a subsidiary of Monsanto.[1] While employed

[1] Monsanto is now owned by Bayer. For simplicity, the Court will refer to Xiang's former employer as Monsanto.

by Monsanto, Xiang reportedly worked on a "component of a digital, on-line farming software platform … referred to as a Nutrient Optimizer." (ECF No. 16 at ¶ 5. The Indictment alleges that "Monsanto and TCC considered the Nutrient Optimizer to be confidential, proprietary information and a highly valuable trade secret as defined in 18 U.S.C. § 1839(3)." (ECF No. 16 at ¶ 15) Broadly speaking, the Indictment alleges that Xiang committed eight separate federal felonies related to the Nutrient Optimizer trade secret. Count One charges him with conspiracy to commit economic espionage, in violation of 18 U.S.C. § 1831(a)(5). Counts Two through Four allege substantive counts of economic espionage and attempted economic espionage, in violation of 18 U.S.C. §§ 1831(a)(1), (a)(3) and (a)(4). Count Five charges Xiang with conspiracy to commit theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(5). Counts Six through Eight allege substantive counts of theft of trade secrets and attempted theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(1), (a)(2), (a)(3), and (a)(4).

On February 19, 2021, Xiang filed a detailed motion to suppress evidence obtained following a warrantless search of his electronic devices. As detailed below, federal agents seized Xiang's devices on June 10, 2017, as he was boarding an international flight from Chicago O'Hare International Airport, with a final destination in China. In his motion to suppress, Xiang advances three primary arguments: (1) a warrant was required to search his devices; (2) the authorities lacked reasonable suspicion to support a warrantless search of his devices; and (3) any search of his devices exceeded any justification of a border search and violated his Fourth Amendment rights.

The government counters that the search of Xiang's devices did not require warrants or probable cause because they were searched pursuant to the long-recognized border search exception to the Fourth Amendment's warrant requirement. The government further contends

that the initial review of information was supported by reasonable suspicion and consistent with the border search exception. Finally, the government notes that a detailed search was only completed after agents applied for and obtained a search warrant.

On May 17, 2021, the undersigned held an evidentiary hearing on Xiang's suppression motion. Xiang was present and represented by Vadim Glozman and Eric Selig. The government was represented by AUSAs Matthew Drake and Gwendolyn Carroll. The government presented the testimony of FBI Special Agent Jaret Depke and Customs and Border Protection Officer Arthur Beck, Jr. (See ECF No. 109). The government also introduced the following exhibits: a travel manifest for Xiang (Gov't Exh. 1); a summary of Xiang Google searches (Gov't Exh. 2); Xiang's termination contract with Monsanto/TCC (Gov't Exh. 3); a receipt for detention of property (Gov't Exh. 4); a Customs and Border Protection Report of June 10, 2017, emailed to SA Depke (Gov't Exh. 5); and a copy of Customs and Border Protection Directive 3340 (Gov't Exh. 6). (See ECF No. 110)

At the conclusion of the hearing, the parties requested an opportunity to submit post-hearing memoranda, which have now been filed. (ECF Nos. 114, 115)

Based on the testimony and evidence adduced at the evidentiary hearing, having had the opportunity to observe the demeanor and evaluate the credibility of the witnesses, and having fully considered the parties' arguments and written submissions, the undersigned makes the following findings of fact, conclusions of law, and recommendations.

FINDINGS OF FACT – SEARCH OF XIANG'S ELECTRONICS

Jaret Depke is a Special Agent ("SA") with the FBI and has been so employed for about seventeen years. Prior his current employment, SA Depke was an officer in the United States Navy for about seven years. For the last fifteen years, SA Depke has been assigned to a Foreign

Counterintelligence team at the FBI.

Arthur Beck, Jr., is a U.S. Customs and Border Protection ("CBP") Officer and a Task Force Officer with the Joint Terrorism Task Force at the FBI office in St. Louis, MO. Officer Beck testified that crimes involving economic espionage are among the laws CBP is charged with enforcing, and that "one of our big priorities … is that we are charged to protect our nation's revenue." (Tr. at 103) Officer Beck also explained that CBP previously encountered tech manuals leaving the country, but now, such information is stored on electronic devices.

According to the Indictment, Xiang is a citizen of the People's Republic of China who was formerly a permanent legal resident of the United States. Xiang worked for Monsanto in the Eastern District of Missouri. According to Xiang's Motion to Suppress, in late May 2017, he notified Monsanto that he intended to resign.

On June 5, 2017, Anne Luther, a Senior Investigator with Monsanto's Global Security Team, contacted SA Depke and requested a meeting to discuss Xiang. SA Depke met with Ms. Luther and others from Monsanto. SA Depke was informed that Xiang was a Senior Research Applications Engineer for Monsanto/TCC. Monsanto advised SA Depke that Xiang had submitted his resignation and that Monsanto had scheduled an exit interview with Xiang for June 9, 2017. SA Depke testified that Monsanto had a group of IT professionals who conducted a review of Xiang's computer usage. SA Depke was informed that Xiang had conducted some suspicious Google searches relative to providing information to a third party, had sent packets of information to a Chinese competitor called Nercita, and had sent confidential Monsanto information from his work e-mail to a personal e-mail account.

Monsanto also advised SA Depke that Xiang had significant communications with a former Monsanto/TCC employee named Jiunnren Chen. Chen and Xiang previously worked on

the same team at Monsanto. SA Depke testified that he was familiar with Chen from a prior investigation in which Chen interviewed for and accepted a job with China National Seed, a direct competitor with Monsanto. According to SA Depke, Chen downloaded 63 documents containing Monsanto's trade secrets to a personal cloud account prior to leaving Monsanto, and he also sent e-mails containing Monsanto confidential information from his work account to a personal e-mail account.

Monsanto representatives did not know what information was included in the packets sent to Nercita or what the communications with Chen entailed.

At some point, SA Depke learned that Xiang lived with his wife in the St. Louis area and that his wife also worked for Monsanto.

On June 8, 2017, SA Depke met with Ms. Luther and several other Monsanto employees. SA Depke learned that, in 2008, Monsanto's security team became aware that Xiang had misrepresented his affiliation with Monsanto/Climate Corporation to an imaging and analysis company named Spectir. According to SA Depke's testimony, the misrepresentation involved Xiang identifying himself as a student and not a Monsanto scientist.

Special Agent Depke was also informed that Xiang told Monsanto he was leaving to work for an agricultural start-up company called "Ag-Sensus," a remote-sensing agriculture company based at the University of Illinois with a professor who was Xiang's PhD advisor.

After meeting with Monsanto, SA Depke contacted Arthur Beck, Jr., an Officer with U.S. Customs and Border Protection. SA Depke considered the case to be a national security investigation involving potential theft of trade secrets, and he provided Officer Beck with information regarding Xiang.

Based on the information provided to him, Officer Beck placed a "Travel Notification"

on Xiang and learned that Xiang was scheduled to travel to China on June 10, 2017. Officer Beck testified that he provided "the articulables" to an officer named Swiatek (in Chicago). (Tr. at 102) Officer Beck testified that the fact that Xiang was leaving Monsanto to work for a start-up was an important consideration to him. (See Tr. at 104)

At the evidentiary hearing, Government's Exh. 1 was a copy of a "Travel Reservation Detail," dated June 8, 20217. Exhibit 1 indicated that Xiang was scheduled to depart Chicago O'Hare International Airport at 8:50 a.m. on June 10, 2017, and travel to Pu Dong Airport in Shanghai, China, via Toronto, Canada. Xiang had a one-way ticket and was travelling alone.

Officer Beck testified that, based on the information provided to him, he believed that Xiang may pose a national security threat and it was CBP's decision to subject Xiang to an inspection at Chicago O'Hare International Airport on June 10, 2017. In the context learning that Xiang may have taken Monsanto proprietary information, Officer Beck explained that a typical scenario that CBP encounters involves people who resign their employment and then leave the United States on a one-way ticket. He described that as a "red flag" scenario for CBP. (Tr. at 109-10)

Officer Beck also advised SA Depke of CBP's inspection, interview, and border search capabilities. SA Depke testified that, prior to consulting with Officer Beck, he was not aware of CBP's ability to detain electronics. SA Depke testified that it was ultimately CBP's decision to conduct any border search of Xiang's electronics. As discussed below, CBP seized Xiang's electronic devices but FBI personnel conducted the eventual search of those devices.

As noted above, Xiang was scheduled for an exit interview at Monsanto on June 9, 2017. The interview occurred and afterwards Monsanto employees reported to SA Depke that Xiang appeared nervous at points during the process. For example, Xiang reportedly appeared nervous

when asked about his prior suspicious Google searches and when reviewing certain documents.

Monsanto provided SA Depke with copies of Xiang's suspicious Google searches (see Gov't Exh. 2) and Xiang's Termination Contract (see Gov't Exh. 3). At the evidentiary hearing, SA Depke's testimony regarding exactly when he received a copy of the Google searches varied. Ultimately, upon having his recollection refreshed, SA Depke testified that he received a copy on June 9, 2017. (Tr. at 83-84) To the extent Xiang disputes that date, the undersigned credits SA Depke's testimony in this regard and finds that SA Depke possessed copies of those searches before June 10, 2017. It is not disputed, however, that the allegedly suspicious Google searches were made on different dates in 2015 and 2016, not in 2017. (See Gov't Exh. 2)

Xiang's Termination Contract included a provision in which Xiang certified that he had not taken or kept any company property, including records and documents, and that he agreed to preserve the confidentiality of all company information, including trade secrets. The Termination Contract also indicated that Xiang was leaving to work for Ag-Sensus, LLC, as co-founder and chief scientist. (See Gov't Exh. 3) Monsanto reported to SA Depke that Xiang appeared nervous and deceptive when he reviewed the Termination Contract.

Xiang rented a car in St. Louis on June 9, 2017, and travelled to Chicago, dropping the car off at the airport on June 10th. CBP officers confronted Xiang on the jetway at O'Hare International Airport and referred him for an interview. Both Officer Beck and SA Depke testified that CBP made the decision to stop Xiang and to seize his electronics for further examination.

Government's Exhibit 5 is a copy of an e-mail thread which summarizes CBP's interactions with Xiang on June 10, 2017, and the disposition of Xiang's electronic devices. Page 2 of Gov't Exh. 5 is an e-mail, dated June 10, 2017, from CBP Officer Randy Swiatek in

Chicago to a person named Noreen Heffernan at an FBI e-mail address,[2] directing that Xiang's detained electronic devices be sent to FBI St. Louis, "Attn: CBP JTTF TFO Arthur Beck and SA Jaret Depke." Page 1 of Gov't Exh. 5 is an e-mail, dated June 12, 2017, from Officer Beck to SA Depke with a formal summary of the CBP inspection. The summary reflects, among other things, that Xiang represented that he was traveling alone to China for one month to visit family. Xiang reported that he was a scientist who, until one-week prior, worked as a researcher for Monsanto. Xiang left Monsanto to work with a start-up, Ag-Sensus, with his former PhD advisor Lei Tan, a professor at the University of Illinois. The report reflects that Xiang's electronic devices were detained at the request of CBBP/FBI JTTF St. Louis and turned over to Officer Swiatek. Xiang was allowed to board his flight. Exhibit 5 also represents that a supervisor named Tejeda witnessed or was notified.

Government's Exhibit 4 is a copy of a Department of Homeland Security "Detention Notice and Custody Receipt for Detained Property" (DHS Form 6051D), with a document number of 1305999. Exhibit 4 reflects that the five items were detained from Xiang, namely a Lenovo Laptop, a Samsung Galaxy, a flash drive, an AT&T SIM card, and a 4G LTE SIM card. The form indicates that the items were detained for an outbound border search exam. The chain of custody portion of Exhibit 4 reflects that the items were transferred to CBP Officer Swiatek on June 10, 2017, and that SA Depke took custody on June 13, 2017. Based on testimony at the hearing, the items were transferred from CBP in Chicago to Officer Beck and SA Depke in St. Louis. When the devices arrived in St. Louis, Office Beck was out, and SA Depke signed for the items.

[2] SA Depke's testimony indicated that the devices were taken to the FBI's Joint Terrorism Task Force Squad located at Chicago O'Hare Airport.

Government's Exhibit 6 is a copy of U.S. Customs and Border Protection Directive No. 3340-049, with a date of August 20, 2009, and a review date of August 2012. The subject of the directive is "BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION." Exhibit 6 reflects the CBP policy in place as of June 10, 2017.[3] The policy "[e]xcludes … actions taken to determine if contraband is concealed within the device itself." (Id. at ¶ 3.4) The policy directs that searches are normally to be conducted in the presence of the person whose devices are being examined, but excludes certain situations, including where there are "national security, law enforcement, or other operational considerations …." (Id. at ¶ 5.1.4) The policy directs that officers are to respect potential confidential business information and restrict the handling of such information. (Id. at ¶ 5.2.3) The policy also contemplates detaining devices for a more comprehensive review. Paragraph 5.3.1 provides that "[t]he search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days." Paragraph 5.3.1.1 summarizes an approval process for continuing a border search after the individual leaves the port or place of detention. Paragraph 5.3.2 and subsidiary paragraphs provide for obtaining assistance from federal agencies outside of CBP or Immigration and Customs Enforcement, including obtaining subject-matter assistance. Supervisory approval

[3] The policy was apparently updated in 2018 in Directive 3340-049A. See Alasaad v. Mayorkas, 988 F.3d 8, 13 (1st Cir. 2021) (citing https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Complaint.pdf). Alasaad is discussed below. The 2018 update "distinguishes between 'basic' and 'advanced' searches, [and] defines an 'advanced search' as 'any search in which an Officer connects external equipment through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents.'" Id. (footnote omitted). Per the 2018 Directive, advanced searches may only be conducted when "there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern." Id. (internal quotations omitted).

is required when subject-matter assistance is requested, and transfers of property for such assistance must be recorded on Form 6051D. (Id. at ¶ 5.3.2.4)

Both SA Depke and Officer Beck testified that Xiang's detained devices were turned over to the FBI to complete the border search examination. CBP requested the subject-matter assistance of the FBI in St. Louis because the potential victim, Monsanto, was located in St. Louis. SA Depke explained why a transfer to St. Louis was more efficient; according to SA Depke, had the items been searched in Chicago, "if any type of intellectual property or trade secret information was found, … it would have to be transported physically from Chicago to St. Louis so that [Monsanto] could actually review the material." (Tr. at 36) Further, SA Depke and the FBI in St. Louis had an established relationship with Monsanto and would be able to identify more expeditiously anything suspicious. The testimony at the hearing also indicated that the investigators expected some of the records would be in Mandarin. SA Depke also testified that he communicated with Officer Beck regarding approvals or authorizations for keeping the devices for more than five days, and that he believed they had the approvals. (See Tr. at 65)

Consistent with the information included on Gov't Exhs. 4, 5, and 6, SA Depke testified that Xiang's electronic devices were transferred from Chicago to the FBI in St. Louis, via FedEx, and received on June 13, 2017, and the transfer was documented on DHS Form 6051D.

Upon receiving the devices, SA Depke conferred with FBI legal counsel and the U.S. Attorney's Office to confirm that FBI officials could search and review the items seized from Xiang under the border search exception. Upon receiving confirmation, on June 14, 2017, the devices were turned over to an FBI Computer Analysis Response Team ("CART") for imaging. The imaging process was completed as of June 20, 2017.

Special Agent Depke testified that, immediately after the imaging process was complete,

he conducted a preliminary keyword search review using terms such as, for example, "[p]roprietary, trade secret, intellectual property, confidential." (Tr. at 39-40) SA Depke quickly identified six documents that he suspected contained Monsanto trade secrets or intellectual property. All of the records were located on an SD card that was found inside the Lenovo Laptop seized from Xiang in Chicago on June 10, 2017. SA Depke printed copies of the six suspect documents and set up a meeting the next day with Monsanto representatives, who confirmed that all six documents contained trade secret or intellectual property.

After receiving confirmation from Monsanto, SA Depke began work on a search warrant application for Xiang's electronic devices. SA Depke testified that the application process took more time than normal because he was required to coordinate with officials at the Department of Justice due to the nature of the investigation.[4] On July 27, 2017, SA Depke applied for and received a warrant to search the devices.[5]

At the evidentiary hearing, SA Depke testified that, prior to his involvement with Xiang, he had received training regarding the PRC and its government's role in economic espionage. SA Depke testified that he was aware of the PRC's initiatives and plans to upgrade their industry, including the agricultural sector. SA Depke referred to these plans as Five Year and Twenty-Five Year Plans. SA Depke also testified that he was aware of another PRC program known at the "Thousand Talents Program." According to SA Depke, the Thousand Talents

[4] Special Agent Depke explained that the FBI considered the investigation to be a "national security matter" and that he was required to work through the "Counterespionage Section" at the Dept. of Justice in Washington, D.C. (See Tr. at 67-68)

[5] At the evidentiary hearing, SA Depke acknowledged that some of the date information in the affidavit for the warrant was incorrect. Correcting the date information would not alter any probable cause analysis. Furthermore, Xiang does not challenge the warrant itself. Rather, Xiang's contention is that the evidence should be suppressed because the initial seizure and the border search of his devices was unconstitutional.

Program involved recruiting "individuals who have knowledge of, or access to[,] foreign technology or intellectual property. And [the Chinese government] also provide financial incentive[s] … for people [who] are outside of China to transfer intellectual property or foreign technology." (Tr. at 43) SA Depke made clear, however, that prior to June 10, 2017, he did not know whether Xiang participated in any of these PRC programs, but his training in this area helped him know what to look for during any search.

Additional findings of fact are included in the discussion below.

DISCUSSION, CONCLUSIONS OF LAW, AND RECOMMENDATIONS REGARDING SEIZURE AND SEARCH OF XIANG'S ELECTRONIC DEVICES

It is not disputed that federal law enforcement seized Xiang's electronic devices, imaged those devices, and conducted keyword searches of at least some of the images, all without first obtaining a warrant. And Xiang did not consent to any seizure or search. Xiang contends that the evidence obtained from his devices must be suppressed for several reasons. Xiang first argues that a warrant was required to image and search Xiang's electronic devices. He argues that the nature of the devices demands a warrant and that the search was not truly a border search at all. In the alternative, Xiang argues that, even if a warrant was not required, the investigators in this case lacked reasonable suspicion. Finally, Xiang argues that any search of his devices was constitutionally unreasonable. The government counters that the search falls within the border search exception.

To resolve Xiang's motion to suppress, our Court must consider the following issues:

(1) Did the initial seizure and subsequent search of Xiang's electronic devices fall within the border search exception to the Fourth Amendment?

(2) If the border exception applies, what level of suspicion, if any, was required?

(3) Was the search reasonable under the Fourth Amendment?

I. Legal Background – Border Searches

The Fourth Amendment shields individuals from unreasonable searches and seizures by law enforcement. United States v. Ramirez, 676 F.3d 755, 759 (8th Cir. 2012). "Reasonableness is always the touchstone of Fourth Amendment analysis, and reasonableness is generally assessed by carefully weighing the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." United States v. Lewis, 864 F.3d 937, 945 (8th Cir. 2017) (quoting County of Los Angeles v. Mendez, 137 S. Ct. 1539, 1546 (2017)). In general, a warrantless search or seizure of a person or that person's effects is unreasonable unless the government shows that the search or seizure "falls within one of a carefully defined set of exceptions." United States v. Anderson, 688 F.3d 339, 343 (8th Cir. 2012) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 474 (1971)).

One of the oldest exceptions to the Fourth Amendment's warrant requirement involves searches and seizures conducted at an international border, which stems from the United States' strong interest "in preventing the entry of unwanted persons and effects." United States v. Flores-Montano, 541 U.S. 150, 152 (2004) (commenting that the "Government's interest" in this regard "is at its zenith at the international border"). Thus, "[s]ince the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." United States v. Montoya de Hernandez, 473 U.S. 536 537 (1985) (citing United States v. Ramsey, 431 U.S. 606, 616-17 (1977)); see also Flores-Montano, 541 U.S. at 152-53 (remarking that "[t]ime and again, we have stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to

protect itself by stopping and examining persons and property crossing ion this country, are reasonable simply by virtue of the fact that they occur at the border'") (quoting Ramsey, 431 U.S. at 616); United States v. Oyekan, 786 F.2d 832, 835 (8th Cir. 1986).[6] Indeed, "routine searches" of persons and their effects "are not subject to any requirement of reasonable suspicion, probable cause, or warrant." Montoya de Hernandez, 473 U.S. at 537 (citations omitted).

A. Routine vs. Non-Routine Border Searches and Electronic Devices

The forgoing summary invites an inquiry into what types of searches should be considered "routine" and whether a different standard applies to "non-routine" border searches. To date, neither the Supreme Court nor the Eighth Circuit has clearly identified what separates routine and non-routine border searches. In Montoya de Hernandez, the Supreme Court found that reasonable suspicion justified a sixteen-hour detention of a traveler suspected of alimentary canal drug smuggling. See 473 U.S. at 544. But the Court did not specify bright line rules or categories for deciding when reasonable suspicion is required.

After at least Montoya de Hernandez, some courts look at the level of intrusiveness of the search or detention as a means of distinguishing between routine and non-routine border searches, that is, which searches may be carried out absent any suspicion, and which searches require particularized suspicion. Some circuits focus on intrusions involving a person's body as

[6] While the law concerning border searches often focuses on inbound persons and containers, the border search exception has been equally applied to the outbound context. See United States v. Baxter, 951 F.3d 128, 135 & n.15 (3d Cir. 2020) ("Consistent with every Court of Appeals to have considered the issue, we concluded that the traditional rationale for the border search exception applies as well in the outgoing border search context.") (citations and internal quotations omitted); United States v. Boumelhem, 339 F.3d 414, 420-21 (6th Cir. 2003) (citation omitted). Similarly, international airports like Chicago's O'Hare constitute a border. See Almeida-Sanchez v. United States, 413 U.S. 266, 272-73 (1973); United States v. Udofot, 711 F.2d 831, 840 (8th Cir. 1983).

opposed to property, while other circuits look at intrusion in broader privacy terms rather distinguishing between a person's body and their property. See, e.g., United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (noting a distinction between intrusions of a person's body versus intrusions involving property); United States v. Levy, 803 F.3d 120, 123 n.3 (2d Cir. 2015) ("Like the Supreme Court … we have suggested that the label 'non-routine' should generally be reserved for intrusive border searches of the person (such as body-cavity searches or strip searches), not belongings.") (citations omitted); Tabbaa v. Chertoff, 509 F.3d 89, 100-01 (2d Cir. 2007) (distinguishing routine and non-routine border searches based on the level of intrusion into a person's privacy); United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1991) (explaining that non-routine border searches are those that impose serious invasions of privacy and embarrass or offend average travelers). The delay caused by, and the complexity of, the seizure and search are not necessarily determinative of whether the matter was routine or non-routine. See Flores-Montano, 541 U.S. at 155-56 (holding that the border search exception permits the government "to remove, disassemble, and reassemble a vehicle's fuel tank" without any showing of individualized suspicion, but also noting the possibility that a search might be so destructive that it could compel a different result).

B. Border Searches of Digital Devices

To date, neither the Supreme Court nor any of the circuits have held that electronic devices such as cell phones should be removed from the border search exception. And to date, neither the Supreme Court nor the Eighth Circuit have addressed the question of whether and under what circumstances border searches of electronic devices require a showing of reasonable suspicion or must comply with additional requirements that are not normally applied in the border search context.

Further complicating matters, the circuits are split on the standards to be applied to forensic border searches of electronic devices such as laptops and cellphones. Broadly speaking, the circuits draw a distinction between manual or basic searches (e.g., searches conducted by manually reviewing the contents of electronic devices) and forensic or advanced searches (e.g., searches conducted using forensic tools). In other words, manual searches are "routine" border searches, and forensic searches are "non-routine" border searches. While there may be meaningful differences between terminology in some cases, for present purposes the terms "manual search" and "basic search" are used interchangeably, and the terms "forensic search" and "advanced search" are used interchangeably.

The First, Fourth, and Ninth Circuits have held that manual/basic searches may be conducted without any suspicion, but forensic/advanced searches require the government to have individualized suspicion. The Fourth and Ninth Circuits also require that any forensic/advanced search be related to one of the core reasons underlying the border search exception, which the undersigned generally refers to as a nexus or purpose requirement. The Ninth Circuit has a strict nexus requirement whereas the Fourth Circuit's nexus requirement has more leeway. The First Circuit considered but rejected a strict nexus requirement. The Seventh Circuit issued a decision that explains that a reasonable suspicion standard applies to non-routine searches, but also found that the government acted in good faith that a warrantless border search did not violate the Fourth Amendment. The Eleventh Circuit has concluded that the government need not have any heightened level of suspicion to justify a border search of electronic devices, including non-routine forensic searches.

In the following sections, the undersigned summarizes the standards applied by the various circuits that have addressed warrantless searches of electronics seized at the border. The

summary starts with the Ninth Circuit, which applies the most stringent standards, and concludes with the Eleventh Circuit, which applies the most lenient standards.

1. Ninth Circuit – *Cotterman* and *Cano*

In United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013) (en banc), cert. denied, 571 U.S. 1156 (2014), the Ninth Circuit held that a forensic examination of a child pornography suspect's computer, conducted as part of a border search, "required a showing of reasonable suspicion." In Cotterman, "[a]gents seized Cotterman's laptop at the U.S.-Mexico border" based on a child molestation report. An initial search uncovered incriminating evidence. See id. at 956. The laptop was transported 170 miles away for "a comprehensive forensic examination" that uncovered child pornography. See id. No warrant was obtained prior to the forensic exam. The en banc Ninth Circuit split, with the majority explaining that, although the government's interests are at their zenith at the border, it does not follow that "anything goes." Id. at 960 (citation omitted). The majority reviewed the caselaw involving intrusive border searches and found that "the key factor triggering the requirement of reasonable suspicion" was "the comprehensive and intrusive nature of a forensic examination—not the location of the examination." Id. at 962 (citation omitted). The majority decision rested largely on the unique "nature of the contents of electronic devices," id. at 964, contrasting routine but destructive searches that have "minimal or no impact beyond the search itself[,] and little implication for an individual's dignity and privacy interests," with "the uniquely sensitive nature of data on electronic devices." Id. at 966.[7]

In United States v. Cano, 934 F.3d 1002 (9th Cir. 2019), cert. denied, 2021 WL 2637990

[7] The Ninth Circuit applied traditional reasonable suspicion standards and concluded that the district court erred in suppressing the evidence at issue. Id. at 968-70.

(June 28, 2021), the Ninth Circuit extended the logic of Cotterman, which involved a laptop computer, to cellphones. The court also concluded that border searches "must be conducted in enforcement of customs laws." Id. at 1013 (citing United States v. Soto-Soto, 598 F.2d 545, 549 (9th Cir. 1979)) Thus, the Ninth Circuit concluded that a search conducted at the border for general law enforcement purposes, rather than a customs purpose, did not fall within the border search exception. In other words, the Ninth Circuit has a nexus requirement. The Ninth Circuit also found that the reasonable suspicion standard articulated in Cotterman was sufficient. See id. at 1015 (discussing Riley v. California, 573 U.S. 373 (2014) and declining to require a warrant or probable cause for border searches of cell phones).

The facts of Cano illustrate that the Ninth Circuit's nexus requirement is strict. Cano was charged with a drug trafficking offense after a drug detecting dog alerted to Cano's vehicle as he crossed into California from Mexico and CBP officials discovered cocaine hidden in his truck. See id. at 1008. Special Agents with Homeland Security Investigations ("HIS") questioned Cano and manually inspected his cell phone. Thereafter, an agent used a cellphone forensic tool known as "Cellebrite" to conduct a more thorough search of Cano's phone. See id. at 1008-09. The Cellebrite search uncovered evidence related to drug trafficking. The Ninth Circuit found that "[t]here is a difference between a search for contraband and a search for evidence of border-related crimes." Id. at 1017 (explaining that the child pornography uncovered in the Cotterman case was contraband and properly subject to the border search exception). The Ninth Circuit recognized that its decision in this regard was in conflict with the Fourth Circuit's decision in United States v. Kolsuz, 890 F.3d 1043 (4th Cir. 2018) (discussed below), which included a nexus requirement but concluded that "'[t]he justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the

border, but also the prevention and disruption of ongoing efforts to export contraband illegally.'" Cano, 934 F.3d at 1017 (quoting Kolsuz, 890 F.3d at 133 (emphasis in Cano)). Thus, the Ninth Circuit affirmatively held that "border officials may conduct a forensic cell phone search only when they reasonably suspect that the cell phone to be searched itself contains contraband." Id. at 1020.[8]

2. Fourth Circuit – *Kolsuz* and *Aigbekaen*

In United States v. Kolsuz, 890 F.3d 133, 146-48 (4th Cir. 2018), the Fourth Circuit held that a forensic border search of a cell phone is a non-routine search that requires individualized suspicion. The Court did not squarely resolve the question of whether the level of individualized suspicion was satisfied by the reasonable suspicion standard. See id. at 147-48 (finding that the agents had reasonable suspicion which demonstrated good faith under existing precedent).

The defendant in Kolsuz was charged with weapons smuggling offenses. Kolsuz was detained while attempting to board a flight from Dulles International Airport to Turkey after agents found firearms parts in his luggage. Agents confiscated Kolsuz's cell phone "and subjected it to a month-long, off-site forensic analysis." Id. at 136. The Fourth Circuit found the border search exception applied because the principles of national sovereignty that provide the basis for the exception "apply equally to government efforts to 'protect and monitor[] exports from the country' as they do to efforts to control imports." Id. (quoting United States v. Oriakhi, 57 F.3d 1290, 1296-97 (4th Cir. 1995)). Thus, the Fourth Circuit concluded that the search of Kolsuz's cell phone satisfied any nexus requirement because the search "was conducted at least in part to uncover information about an ongoing transnational crime … [so] it fits within the core

[8] The Ninth Circuit ultimately held that the record did not show that agents had reasonable suspicion that Cano's cell phone contained contraband and directed suppression of evidence obtained via the Cellebrite search. Id. at 1021.

rationale underlying the border search exception." Id. at 144 (internal citations and quotations omitted).[9]

In United States v. Aigbekaen, 943 F.3d 713 (4th Cir. 2019), cert. denied, 2021 WL 2637946 (June 28, 2021), the Fourth Circuit applied Kolsuz, finding that a warrantless search of an international traveler's electronic devices was not justified by the border search exception because the search was directed at uncovering evidence of a purely domestic crime, untethered to protecting the integrity of the nation's borders.

The defendant in Aigbekaen was suspected of sex trafficking of a minor in the United States. When the defendant returned to John F. Kennedy International Airport after travelling abroad, agents seized his electronic devices, transported the devices to Baltimore, MD, imaged the devices, and conducted forensic examinations. Id. at 717-18. The defendant was charged with sex trafficking offenses and convicted following a trial. The Fourth Circuit held that the searches were unconstitutional because they did not satisfy the nexus requirement—they were unrelated to the core rationales of the border search exception. See id. at 720-22 ("If a nonroutine search becomes too 'attenuated' from the[] historic rationales, it 'no longer [will] fall under the exception.'") (quoting Kolsuz, 890 F.3d at 143). Nonetheless, the court affirmed the convictions because the search occurred prior to Kolsuz and the agents acted in good faith reliance on existing caselaw. Id. at 725.[10]

---

[9] In other words, unlike the Ninth Circuit in Cano which requires the search to focus on contraband itself, the Fourth Circuit permits border searches for "mere evidence" of a border-related crime. See also Warden v. Hayden, 387 U.S. 294, 301 (1967) (rejecting notion that the Fourth Amendment "supports the distinction between 'mere evidence' and instrumentalities, fruits of crime, or contraband").

[10] Similar to Kolsuz, in Aigbekaen, the Fourth Circuit explained that a forensic border search requires a showing of individualized suspicion, but it declined to decide whether reasonable suspicion satisfied that showing. See id. at 723.

3. First Circuit – *Alasaad*

In Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir.), cert. denied, 2021 WL 2637881 (June 28, 2021), the First Circuit addressed border searches of electronic devices in the context of a civil suit challenging CBP policies. The First Circuit held that routine searches may be conducted without reasonable suspicion, and that even advanced searches do not require a warrant or probable cause. See id. at 17-18.[11] The court rejected the strict nexus requirement articulated by the Ninth Circuit in Cano, instead concluding that a border search may be justified by "a search for evidence of either contraband or a cross-border crime." Id. at 19, 20.[12]

4. Seventh Circuit – *Wanjiku*

In United States v. Wanjiku, 919 F.3d 472 (7th Cir. 2019), Customs officials looking for suspected child sex tourists targeted Wanjiku, a United States citizen who arrived at Chicago O'Hare International Airport from the Philippines. CBP officers conducted a warrantless examination of Wanjiku's digital devices using a forensic preview tool. Id. at 476-78. Thereafter, investigators applied for and obtained a warrant to fully search the devices. The Seventh Circuit rejected Wanjiku's argument that the preview searches required probable cause and a warrant, noting that, in the Seventh Circuit, reasonable suspicion was required for non-routine searches. See id., 483. The court did not clearly determine whether using a forensic preview tool constituted a non-routine search. Rather, the court held that the government acted with a good faith belief that the preview searches did not violate the Fourth Amendment, and

---

[11] Relying on prior circuit precedent, the First Circuit noted that non-routine searches require reasonable suspicion, and the court's analysis at least suggested that advanced or forensic searches of electronic devices were non-routine searches.

[12] The First Circuit described Cano as articulating a "narrow view … [that] fails to appreciate the full range of justifications for the border search exception beyond the prevention of contraband itself entering the country." Id. at 21.

that, at the moment of the search, the officers had reasonable suspicion that a search would reveal evidence of criminal activity involving minors. See id. at 487, 488.

5. Eleventh Circuit – *Touset*

In United States v. Touset, 890 F.3d 1227, 1230 (11th Cir. 2018), information suggested that the defendant was involved in child pornography offenses. When Touset arrived in Atlanta following an international flight, customs officials seized and conducted a forensic search of his electronic devices. Id. Touset unsuccessfully moved to suppress the evidence. On appeal, the Eleventh Circuit stressed that "searches at the border of the country, 'never require probable cause or a warrant.'" Id. at 1232 (quoting United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018)). The Eleventh Circuit further held that no level of suspicion is required for the search of property at the border, even personal electronics. See id. at 1233. The Eleventh Circuit reasoned that "[t]he Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive …." Id. Instead, the court reviewed relevant Supreme Court and circuit precedent and concluded that the reasonable suspicion standard at the border has been reserved "only for highly intrusive searches of a person's body." Id. at 1233-34 (citations and internal quotations omitted). The court considered many of the arguments that animated the Fourth and Ninth Circuits decisions to the contrary, but it found them unpersuasive. The court found no reason to give special treatment to electronic devices simply because "so many people now own them or because they can store vast quantities of records or effects." Id. at 1233. The court was "also unpersuaded that a traveler's privacy interest should be given greater weight than the interests [of the sovereign] in protecting … its territorial integrity." Id. (citations and internal quotations omitted).[13]

[13] The Eleventh Circuit did not directly address any nexus requirement, presumably

II. Analysis of Issues Relative to Search of Xiang's Electronic Devices

With the foregoing principles in mind, the undersigned finds that the detention and review of Xiang's electronic devices falls within the border search rubric. First, the undersigned recommends that our Court reject Xiang's argument that the Supreme Court's decision in Riley dictates that any search of his electronic devices required a warrant. The undersigned has identified no binding or persuasive authority to support Xiang's position in this regard. To the contrary, several circuits have considered and rejected similar arguments.

The undersigned further finds that, at the time of the seizure and through the initial search, CBP and the FBI possessed reasonable suspicion to believe that Xiang had taken Monsanto trade secret information and records, and that such information and records would be found on Xiang's electronic devices. Because the undersigned believes that reasonable suspicion existed, our Court may assume, without necessarily deciding, that SA Depke's keyword searches should be treated as non-routine, forensic/advanced searches, and that such searches require a showing of reasonable suspicion.[14]

A. Does the Border Search Exception Apply to the Investigation?

Xiang argues that the search in his case "was untethered from the underlying justifications of the border search exception." [ECF No. 114 at 4] This tethering argument implies a nexus requirement, similar to the requirements imposed by the Ninth and Fourth

---

because it found that no suspicion whatsoever was required. The Eleventh Circuit found in the alternative that reasonable suspicion supported the forensic searches of the devices seized from Touset at the border.

[14] Under CBP's current policy, as discussed above, the keyword searches would be considered "advanced" because forensic tools were used to image Xiang's devices before SA Depke conducted his searches. CBP policy is not binding on our Court, but it is consistent with substantial circuit caselaw (discussed above) holding that forensic searches are non-routine and require reasonable suspicion.

Circuits. Even assuming that the Supreme Court or the Eighth Circuit would also adopt a nexus requirement, that requirement would be satisfied. The search in this case was related to an investigation involving the possible exfiltration of trade secret information. Unlike the facts confronted by the Fourth Circuit in Aigbekaen, SA Depke and Officer Beck were not considering a purely domestic criminal matter. And stolen trade secrets could reasonably be viewed as akin to the contraband at issue in Kolsuz. Therefore, the undersigned finds that the border search exception applies. Simply stated, even the strict nexus requirement from Cano would be satisfied in this case.

B. Did the Search Require a Warrant?

Xiang argues that, following the Supreme Court's decision in Riley v. California, 573 U.S. 373 (2014), and in light of the rationale underlying the border search exception, a warrant based on probable cause was required to search his electronic devices. In Alasaad, the First Circuit rejected a substantially similar argument.

> In United States v. Riley, 573 U.S. 373 (2014),
>
> > the Supreme Court held that the search incident to arrest exception to the warrant requirement did not extend to searches of cell phones…. In doing so, it reasoned that individuals have a heightened privacy interest in their electronic devices due to the vast quantity of data that may be stored on such devices, and that the government's interests in searching an arrestee's cell phone during an arrest was limited because such searches do not meaningfully advance the search incident to arrests exceptions purposes of protecting police officers and preventing the destruction of interests…. Thus, the balance of interests did not support [applying] the search incident to arrest exception [to cellphones].

Alasaad, 988 F.3d at 17 (citing Riley, 573 U.S. 386, 388-91, 403). Alasaad also recognized that that "[e]very circuit that has faced this question has agreed that Riley does not mandate a warrant requirement for border searches of electronic devices whether basic [e.g., manual] or advanced [e.g., forensic]." Id. at 17-18 (citing Aigbekaen, 943 F.3d at 719 n.4; Cano, 934 F.3d at 1015-16;

Vergara, 884 F.3d at 1311-12). The First Circuit concluded that "Riley did not either create or suggest a categorical rule to the effect that the government must always secure a warrant before accessing the contents of an electronic device." Id. at 17 (cleaned up). That court further explained that the search incident to arrest and border search exceptions serve entirely different purposes. Id.[15]

The undersigned finds the First Circuit's analysis persuasive. In the absence of controlling Supreme Court or Eighth Circuit precedent, therefore, it is recommended that our Court adopt the controlling view, as described in Alasaad, and conclude "that neither a warrant nor probable cause is required for a border search of electronic devices." Id. at 18.

C. Was there Reasonable Suspicion at the Time of Seizure?

Having concluded that a warrant and probable cause are not required, the next issue is what level of suspicion, if any, was required for the seizure and search of Xiang's devices in this case. As explained above, there is a split of authority on this topic. A majority of the circuits that have considered the issue have drawn a distinction between manual or basic searches, which require no suspicion, and forensic or advanced searches, which require some level of individualized suspicion short of probable cause. Because the investigators in this case possessed reasonable suspicion, our Court may presume, without deciding, that the search at issue was a forensic or advanced search that required a showing of reasonable suspicion that Xiang was engaged in criminal activity and evidence of that activity would be located on his electronic devices.

"The concept of reasonable suspicion is not 'readily, or even usefully, reduced to a neat

[15] As the Ninth Circuit also explained, the balance tilts "much more favorably to the Government" when one considers the federal government's critical interest in securing border integrity. Cano, 934 F.3d at 1015 (citing Montoya de Hernandez, 473 U.S. at 538-40).

set of legal rules.'" United States v. Quinn, 812 F.3d 694, 697 (8th Cir. 2016) (quoting Illinois v. Gates, 462 U.S. 213, 232 (1983)). "Reasonable suspicion must be supported by more than a 'mere hunch,' but 'the likelihood of criminal activity need not rise to the level required for probable cause, and it falls considerably short of satisfying the preponderance of the evidence standard.'" Roberts, 787 F.3d at 1209 (quoting United States v. Arvizu, 534 U.S. 266, 274 (2002)). A reviewing court considers the totality of the circumstances. See id. In assessing the reasonableness of the suspicion, officers may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person." Arvizu, 534 U.S. at 273 (internal quotations and citation omitted). The Court may also consider "situational factors" including timing and location information. Roberts, 787 F.3d at 1209. "[E]ven 'a series of acts that appear innocent, when viewed separately, may warrant further investigation when viewed together.'" United States v. Gonzalez, 781 F.3d 422, 428 (8th Cir.) (quoting United States v. Weaver, 966 F.2d 391, 394 (8th Cir. 1992)), cert. denied, 577 U.S. 859 (2015). This totality of the circumstances standard precludes courts from engaging in a "divide-and-conquer" analysis of each fact and circumstance separately. Quinn, 812 F.3d at 698 (citing cases).

By the time CBP detained Xiang's electronics on the morning of June 10, 2017, the FBI and CBP investigators were aware of several key facts and circumstances that, when viewed together, provide sufficient reasonable articulable suspicion to justify a warrantless seizure and forensic search of Xiang's electronics. [16]

[16] "In deciding whether there is reasonable suspicion, an officer may rely on information provided by other officers as well as any information known to the team of officers conducting the investigation." United States v. Guzman, 926 F.3d 991, 997 (8th Cir. 2019) (citations and internal quotations omitted). This is known as the "collective knowledge" rule. In applying the collective knowledge rule, there must be some degree of communication between the officers. See United

No later than June 10, 2017, the investigators knew that Xiang had recently left his employment with Monsanto. Monsanto personnel conducted a review of Xiang's computer usage and learned that, in 2015 and 2016, Xiang conducted several suspicious Google searches which involved terms like "evidence to accuse me," "company information to the third parties," "can use it against me in the future," "I will be cautious," and "cautious are needed." (See Gov't Exh. 2) Monsanto personnel also discovered that Xiang had transferred company information from his company e-mail account to a personal e-mail account. Further, Xiang had been in correspondence with a former employee and colleague, Jiunnren Chen, who SA Depke knew had previously downloaded numerous Monsanto trade secret documents to a cloud account, and sent e-mails containing Monsanto confidential information to a personal e-mail account before leaving the company to work for a Chinese competitor. The FBI was also advised that Xiang had sent packets of information of unknown content to a Chinese competitor of Monsanto named Nercita. (See Tr. at 8-9) The FBI was also informed that Monsanto's security team became aware of Xiang in 2008, when they learned that Xiang, who was then a Monsanto employee, misrepresented himself as a University of Illinois student in an attempt to acquire information about a United States imaging company named Spectir. (See Tr. at 12; Xiang Post-Hearing Brief, ECF No. 114-1 at 1) The FBI knew that Xiang reported that he was going to leave Monsanto and work for a start-up with his former PhD adviser at the University of Illinois. Monsanto further advised the FBI that Xiang participated in an exit interview on June 9, 2017. According to Monsanto representatives, Xiang appeared visibly nervous during the exit interview when he was confronted with his suspicious Google searches and when he reviewed

---

States v. Shackleford, 830 F.3d 751, 753 (8th Cir. 2016) (citation omitted). The record in this matter demonstrates a sufficient degree of communication between the FBI and CBP, including CBP officers in Chicago. The collective knowledge rule applies.

his termination agreement, which discussed his obligations regarding Monsanto's intellectual property. CBP and the FBI also knew that, just one day after his exit interview, Xiang was scheduled to leave the country and travel to China, on a one-way ticket, without his family. The timing of Xiang's travel, the fact that he was travelling alone on a one-way ticket, and the fact that he was departing from Chicago, were significant situational factors when viewed in the totality of the circumstances. Finally, when he was confronted at the international airport, Xiang was in possession of numerous electronic devices.[17]

Xiang takes strong aim at many of these facts and circumstances. Xiang provides arguably innocent explanations for several of the facts the government relied upon to justify its actions. For example, Xiang explained that his one-way travel resulted from using airline miles to pay for his ticket, and that he stated that was travelling to visit his family. Xiang also notes that he consistently reported that he left Monsanto to work for a former advisor, at a start-up company based in Illinois. The suspicious Google searches were conducted a year or two prior to June 2017, and neither Monsanto nor any of the government investigators knew what information was exchanged between Xiang and his former colleague, Chen.

Many of Xiang's points would have some persuasive force if viewed in isolation. But such an approach ignores the appropriate standard of review. While no single fact alone may be enough to establish reasonable suspicion, our Court considers the totality of the facts and circumstances and must not consider each fact in isolation. See Quinn, 812 F.3d at 698; Roberts, 787 F.3d at 1209. And we must also consider the possibility that facts which may seem innocent on their face may take on a different meaning to someone with specialized training, experience,

[17] SA Depke also had specialized knowledge and training concerning efforts by the PRC to obtain foreign intellectual property. This training, coupled with the initial information from Monsanto, supports treating the matter as a national security concern.

or who has the benefit of additional information. See Arvizu, 534 U.S. at 273; Gonzalez, 781 F.3d at 428.

When viewed in their totality, the undersigned finds that SA Depke and CBP officers possessed sufficient reasonable suspicion to justify a non-routine, forensic/advanced search of Xiang's electronic devices. In reaching this conclusion, the undersigned has given weight to facts and circumstances provided to SA Depke from Monsanto. SA Depke was entitled to rely on Monsanto for several reasons. First, Monsanto is a known entity and SA Depke personally spoke and met with its employees, and those employees could be held accountable for providing false information to SA Depke. See United States v. Knutson, 967 F.3d 754, 758 (8ht Cir. 2020). Second, SA Depke was able to corroborate some of the information and suspicions Monsanto provided. See United States v. Mays, 993 F.3d 607, 615 (8th Cir. 2021). For example, he obtained a copy of the suspicious Google searches. SA Depke also learned that Xiang was scheduled to leave the United States, on a one-way ticket, only one day after his exit interview.

Finally, Xiang correctly observes that, in assessing reasonable suspicion, the Eighth Circuit has sometimes given diminished weight to a person's perceived nervousness. See, e.g., United States v. Jones, 269 F.3d 919 (8th Cir. 2001). Xiang's reliance on cases such as Jones is arguably misplaced because such cases are factually distinguishable. Jones involved a traffic stop that was extended. The Eighth Circuit observed that, although "a person's nervous behavior may be relevant, [courts should be] wary of the objective suspicion supplied by generic claims that a Defendant was nervous or exhibited nervous behavior after being confronted by law enforcement officials." Id. at 928-29 (citation and internal quotations omitted). The Court reasoned that "many motorists become nervous when pulled over and confronted by law enforcement officials." Id. at 929. In contrast, Xiang became visibly nervous during an exit

interview, not conducted by law enforcement, when confronted with specific facts and issues. In other words, this case does not involve generic claims of nervousness. Xiang's nervousness in that situation is relevant in assessing the likelihood that he might have taken company secrets. To be clear, the undersigned has given weight to Monsanto's report that Xiang was nervous, but also finds that there would be reasonable suspicion even if Xiang's reported nervousness were not considered.

In summary, having considered the totality of the facts and circumstances in the record, the undersigned finds that, as of the morning of June 10, 2017, CBP and FBI personnel possessed sufficient reasonable suspicion to conclude that Xiang's electronic devices contained Monsanto trade secret information.

D. Was the Search Constitutionally Reasonable?

Xiang also argues that the evidence should be suppressed because the search was unreasonable and violated CBP policy.

1. FBI Involvement

A substantial component of Xiang's argument focuses on a contention that CBP was not truly involved and was acting at the behest of the FBI. But how and why CBP became involved is not controlling. Xiang has identified no relevant law or analogous cases to support his premise. To the contrary, "[w]hether a Customs official's reasonable suspicion arises entirely from her own investigation or is prompted by another federal agency is irrelevant to the validity of a border search, which … does not depend on whether it is prompted by a criminal investigative motive." United States v. Levy, 803 F.3d 120, 123 (2d Cir. 2015) (citations and internal quotations omitted). In Levy, the Second Circuit noted with approval the fact that FBI agents "frequently assist customs officials in the execution of border searches." Id. (citations and

internal quotations omitted). Similarly, the Sixth Circuit rejected an argument that a border search was a pretext to circumvent the warrant requirement and, therefore tainted and unconstitutional because the FBI participated in or directed the search. See United States v. Boumelhem, 339 F.3d 414, 423 and n.7 (6th Cir. 2003).

The facts and circumstances from the evidentiary hearing establish that the FBI was no doubt leading an investigation of Xiang that was initiated after SA Depke received information from Monsanto. The undersigned credits the testimony of SA Depke and Officer Beck that CBP, and not the FBI, made the ultimate decisions about whether Xiang was going to be stopped and whether his devices were to be seized. Again, there is no doubt that the FBI had a keen interest in seizing and searching Xiang's devices, but SA Depke credibly testified that he was not aware of the scope of CBP's ability to seize electronic devices at the border. And Officer Beck's testimony and the relevant documents from the encounter with Xiang on June 10, 2017, support a finding that it was CBP's call as to whether Xiang would be stopped and whether his devices would be seized.

The undersigned finds that the FBI's participation and role in the investigation did not render the border search constitutionally unreasonable.

2. Delay in Completing Search

To the extent Xiang's reasonableness arguments also embrace a challenge to the duration of the review, the undersigned finds that CBP and the FBI acted with reasonable diligence. First, there is no set or firm constitutional time limit for completing a border search. See Alasaad, 988 F.3d at 21 (citing Montoya de Hernandez, 473 U.S. at 544). In this case, it was reasonable in the circumstances to transfer the devices to St. Louis to complete the border search examination. That transfer required about three days. It was also reasonable to image the devices to preserve

their integrity before conducting any search. The imaging process took several days. The record further indicates that, once images were available, SA Depke promptly conducted simple keyword searches to confirm or dispel his suspicions. SA Depke's keyword searches uncovered documents he suspected contained victim intellectual property, which he promptly conveyed to Monsanto and confirmed his suspicions. Armed with that information, SA Depke applied for and obtained a search warrant.

The record indicates that there was a month-plus delay from the time SA Depke's keyword searches confirmed his suspicion until the time he applied for and obtained a search warrant for the devices.

The fact that SA Depke sought a warrant upon confirming his suspicious was certainly reasonable. As for the delay, the Eighth Circuit recently explained that courts are to balance privacy concerns against law enforcement concerns when assessing the reasonableness of any delay in seeking a search warrant following the warrantless seizure of property such as a laptop. See Mays, 993 F.3d at 617 (citing United States v. Laist, 702 F.3d 608, 613 (11th Cir. 2012)).[18]

In Xiang's case, the nature of the property seized (his electronic devices) weighs in his favor. Further, Xiang did not consent to the seizure of his property. See Mays, 993 F.3d at 617 (discussing non-exhaustive factors). Also, while there is no information suggesting that Xiang or any representative of Xiang requested the return of his devices, the devices were promptly imaged.[19] Thus, any delay did not work meaningful prejudice to Xiang because the images

[18] In Mays, the FBI seized the defendant's laptop from a third-party, without any consent from the defendant. See id. at 613. In Laist, the electronic devices were seized with the defendant's consent, but the consent was revoked several days later. Thus, the devices were arguably obtained lawfully but held without consent pending application of a warrant. See 702 F.3d at 611.

[19] The undersigned is not suggesting that a person must request the return of his property

would have been available to search even if the devices had been promptly returned to Xiang.

The government's interests in this case are stronger than Xiang's. First, as this matter involved a possible attempt to smuggle trade secret information out of the country, the government had a very strong and legitimate interest in holding the devices; indeed, the government's interests were at their "zenith." Flores-Montano, 541 U.S. at 152. The investigation was in its early stages, and involved numerous complex considerations, including the nature of the offense, the number and nature of the electronic devices seized, and the potential for uncovering complex, specialized, and foreign-language evidence during the execution of any search. The undersigned finds that it was reasonable for CBP to transfer the devices to the FBI in St. Louis to leverage the subject-matter expertise and close proximity to the victim, which also ensured that any sensitive information uncovered would remain under a tight chain of custody. It was reasonable for the FBI CART team to first image the devices so that there would be a degree of data integrity. That took time. The testimony and evidence from the evidentiary hearing also established that, once images were available, SA Depke promptly conducted limited key-word searches that were closely tailored to the purpose of identifying Monsanto trade secret and confidential information. SA Depke then promptly conveyed his findings to the subject-matter experts at Monsanto for confirmation. Thereafter, SA Depke took steps to secure a warrant for a more thorough search of Xiang's devices. Regarding the time from when SA Depke confirmed he had probable cause until he actually applied for a warrant,

---

in order to sustain a reasonableness challenge based on delay. Rather, the undersigned is emphasizing that, even if Xiang had requested the return of his property and it was promptly returned, the FBI would have been able to search the images that they had already constitutionally obtained pursuant to the border search exception. Thus, the evidence would have been inevitably discovered. See United States v. Brooks, 715 F.3d 1069, 1075-76 (8th Cir. 2013) (applying inevitable search doctrine to search of cell phone conducted pursuant to a warrant obtained months after an initial seizure and warrantless search of the device).

any such delay was also reasonable. The nature of the offense involved, at least potentially, national security matters involving a foreign government. Thus, while it may not always be appropriate to consider internal government approval processes, the undersigned finds that, in these circumstances, it was reasonable for the investigators and prosecutors in St. Louis to consult with experts at the Department of Justice. On balance, therefore, the undersigned finds that the delay in obtaining the warrant was not constitutionally unreasonable.

3. Administrative / Procedural Irregularities

The undersigned also does not believe that Xiang has shown any search was constitutionally unreasonable because the CBP failed to follow its own procedures. Xiang offers limited legal authority for his premise that a failure to follow administrative procedures should result in the suppression of evidence on constitutional grounds. Absent a clear Fourth Amendment violation, Courts normally do not suppress evidence even when federal agents do not follow significant procedural requirements such as those imposed by Rule 41 of the Federal Rules of Criminal Procedure. Furthermore, applying the standards for Rule 41 violations to the alleged administrative violations herein would not call for suppression in Xiang's case.

"A Rule 41 violation is not per se an unreasonable search and seizure in violation of the Fourth Amendment." United States v. Horton, 863 F.3d 1041, 1048 (8th Cir. 2017) (citation and internal quotations omitted), cert. denied, 138 S. Ct. 1440 (2018). The relevant inquiry is whether "the violation was merely technical or instead rises to the level of a violation of the Fourth Amendment." Id. A rule violation "warrants exclusion only when (1) the violation is of constitutional magnitude; (2) the defendant is prejudiced in that the search would not have taken place or would not have been as intrusive; or (3) there is evidence of an intentional and deliberate or reckless disregard for the rule." United States v. Skarda, 845 F.3d 370, 375 (8th

Cir. 2016) (citing United States v. Freeman, 897 F.2d 346, 350 (8th Cir. 1990)). "To determine prejudice, we ask whether the search would have occurred had the rule been followed. If so, there is no prejudice to the defendant." United States v. Hyten, 5 F.3d 1154, 1157 (8th Cir. 1993); see also United States v. Turner, 781 F.3d 374 (8th Cir. 2015) (quoting Hyten).

Xiang has not met the prejudice or reckless disregard standard. Xiang has not provided any meaningful facts to show prejudice to him flowing from the alleged failure to document supervisory approval for seeking subject-matter assistance from the FBI and for the delay in completing the key word searches.

Xiang has also not shown that anyone acted with reckless disregard for the administrative procedures. On this latter point, while the documentary record regarding approvals is thin, Officer Beck testified that he believed the procedures were followed. Relatedly, Gov't Exh. 5 indicates that a Supervisor named Tejeda was involved. And SA Depke credibly testified that he believed that the appropriate approvals had been secured, and before he began the process at the FBI, he sought and obtained legal advice from both his division counsel as well as the U.S. Attorney's Office. The undersigned also finds that it was reasonable for CBP officers to seek subject-matter assistance from SA Depke and investigators in St. Louis. Determining what, if any, records reflect Monsanto trade secrets could only reasonably be accomplished by consulting with Monsanto experts. It was reasonable to transfer the electronic devices to St. Louis so that any suspect records could be more readily shared with those experts at Monsanto. This process would tend to improve the speed and efficacy of the search effort, not detract from it. On these facts, the undersigned finds that SA Depke, Officer Beck, and the CBP arguably complied with the administrative procedures and, even if they did not, they did not act with reckless disregard to

those procedures.[20]

The undersigned finds, therefore, that the border search of Xiang's electronic devices was constitutionally reasonable, even assuming that the administrative procedures were not fully followed or completely documented.

E. Summary of Conclusions Regarding Search of Xiang's Electronic Devices

In summary, the undersigned recommends that the Court deny Xiang's motion to suppress evidence seized from his electronic devices. The undersigned finds that the search of Xiang's devices was constitutional pursuant to the Fourth Amendment's border search exception, that the investigators possessed reasonable suspicion to support an advance or forensic search of Xiang's electronics, and that the search was constitutionally reasonable. Finally, Xiang does not raise an independent challenge to the warrant that SA Depke ultimately obtained. Inasmuch as the initial border search was constitutional, the undersigned finds that the subsequent search warrant was not the fruit of the poisonous tree.

OTHER MOTIONS

I. Xiang's Motion for Early Trial Subpoenas [ECF No. 79]

The government has not opposed Xiang's motion for early return of trial subpoenas,

[20] The undersigned identified one case from the Southern District of Ohio in which evidence was suppressed for failure to follow CBP procedures. In United States v. Laynes, CBP officers briefly detained a Mexican citizen returning to the United States to determine if he needed to be brought before an immigration judge. See 481 F. Supp.3d 657, 659 (S.D. Ohio 2020). During that process, an officer conducted a warrantless manual search of the Google photos folder on Laynes' iPhone and noticed suspected child pornography. Id. at 659-60. The officer, however, failed to first place the iPhone into "airplane mode," as CBP policy required. It was later determined that the suspected child pornography was not on the iPhone but in a cloud account that was accessed via the iPhone. Id. at 661-62. The district court concluded that the failure to follow CBP policy in that case was critical because "border-search authority does not extend to searches of remotely stored information." Id. at 667 (internal quotations and citations omitted). Xiang's case is easily distinguished from the situation in Laynes.

therefore that motion will be granted.

II. Xiang's Motion for Disclosure of Expert Witnesses [ECF No. 95]

At an earlier stage of the pretrial proceedings, the Court and the parties discussed issues relating to the scope of discovery, the scope of the trade secret at issue in the Indictment, and the related need to secure expert witness testimony. Xiang aptly explains that he needs access to expert witness discovery so that he may hire his own expert to rebut the government's expert. Xiang has asked the Court to require the government to provide its expert witness notice now, to avoid the risk of unnecessary and prejudicial delay. The government represents that it has not yet identified or secured an expert witness, but also assures Xiang and the Court that it will do so sufficiently in advance of trial to enable Xiang time to effectively prepare.

There is no trial date set, making it difficult for the Court to fully evaluate this matter. On the other hand, the investigation is four years old, and the case has been pending in our Court for over eighteen months. Therefore, the government is ordered to report to the Court no later than August 27, 2021, when it will provide its expert notice to Xiang. Xiang's motion for early disclosure will be denied without prejudice at this time.

CONCLUSION

Accordingly,

IT IS HEREBY RECOMMENDED that Xiang's Motion to Suppress Evidence [ECF No. 93] be **DENIED**.

IT IS HEREBY ORDERED that Xiang's Motion for Early Return of Trial Subpoenas [ECF No. 79] is **GRANTED**.

IT IS FURTHER HEREBY ORDERED that, no later than August 27, 2021, the government will notify the Court and Xiang the date on which it will provide any expert

notice(s).

IT IS FURTHER HEREBY ORDERED that Xiang's Motion to Require Government to Produce Notice of Expert Witness [ECF No. 95] is **DENIED** without prejudice.

The parties are advised that they have fourteen (14) days in which to file written objections to the foregoing Report and Recommendation and Orders, unless an extension of time for good cause is obtained, and that failure to file timely objections may result in a waiver of the right to appeal questions of fact. Objections must be timely and specific in order to require review by a District Court Judge. See Thompson v. Nix, 897 F.2d 356 (8th Cir. 1990); 28 U.S.C. § 636(b)(1)(A); and Fed. R. Crim. P. 59(a).

The trial of this matter will be set by further order of the Court, before the Honorable E. Henry E. Autrey, United States District Judge.

/s/ *John M. Bodenhausen*
JOHN M. BODENHAUSEN
UNITED STATES MAGISTRATE JUDGE

Dated this 23rd day of July , 2021.